Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 2 (2017), pp. 493-517

http://www.ripublication.com

Genetic Traits of Odd Numbers with Applications in Factorization of Integers

Xingbo Wang

[1] *Department of Mechatronics, Foshan University,*
Foshan City, Guangdong Province, PRC, 528000, China.

Abstract

The article proves that there exist genetic traits among integers: an odd number will regularly transmit its genes to other integers by making itself be a divisor of certain odd composite numbers under definite laws. By the genetic traits, distributive scope of divisors of an odd composite number can be exactly known and limited in a definite range by means of valuated binary tree. Genetic structure, genetic graph and complementary genetic graph are constructed in term of the discovered genetic laws. New approaches for primality test and integer factorization are also put forward with numerical experiments on factorization of some Fermat numbers, Mersenne numbers and other big integers. Experiments indicate that the new approach is averagely faster than the Pollard' Rho approach.

Keywords: Integer factorization, Genetic law, Binary tree, Algorithm design

MSC 2000: 11A51,11A05

I. INTRODUCTION

Studying integers by means of binary tree can reveal many new properties of integers. Article [1] put forward the concept of valuated binary tree and proved some fundamental laws on division relations between the root and other nodes of an odd-number-valuated tree. Article [2], following the study of the article [1], investigated several new properties of odd numbers, including laws of symmetric nodes, symmetric common factors, subtrees' duplication, subtrees' transition, root division

and uniform sum. These properties are called amusing properties by article [2] but in fact they are very serious and important for study of the odd numbers. This article continues revealing an important new property that discloses a genetic trait of factors' transitions among odd numbers. By the genetic traits, distributive scope of divisors of an odd composite number can be exactly known and limited in a definite range that makes it easier to factorize an odd composite number.

II. PRELIMINARIES

2.1 Definitions and Notations

This article continues adopting definitions and notations related with the valuated binary tree and subtrees that were given in [1] and [2]. Odd numbers mentioned in this article are those bigger than 1. If the root of a valuated binary tree is 3, then the tree is called T_3-tree, simply denoted by T_3, as shown in figure 1. Note that each odd number bigger than 1 must be a node of T_3, hence odd number is usually written by its position in T_3. For example, $N_{(k,j)}$ is to indicate the odd number is on the j^{th} position of the k^{th} level in T_3, where $k=\lfloor \log_2 N_{(k,j)} \rfloor -1$. In distinguishing from T_3, symbol $T_{N_{(k,j)}}$ denotes a subtree whose root is $N_{(k,j)}$ (in T_3) and symbol $N_{(i,\omega)}^{N_{(k,j)}}$ denote the node at the ω^{th} position on the i^{th} level in $T_{N_{(k,j)}}$. Node $N_{(i,\omega)}^{N_{(k,j)}}$ and node $N_{(i,2^i-1-\omega)}^{N_{(k,j)}}$ are geometrically symmetric on the i^{th} level thus they are called position-symmetric nodes. It is a convention that any tree's root starts from level 0. Symbol (a,b) or $[a,b]$ in this whole article means a set of consecutive odd numbers that are distributed in the open interval (a,b) or the close interval $[a,b]$.

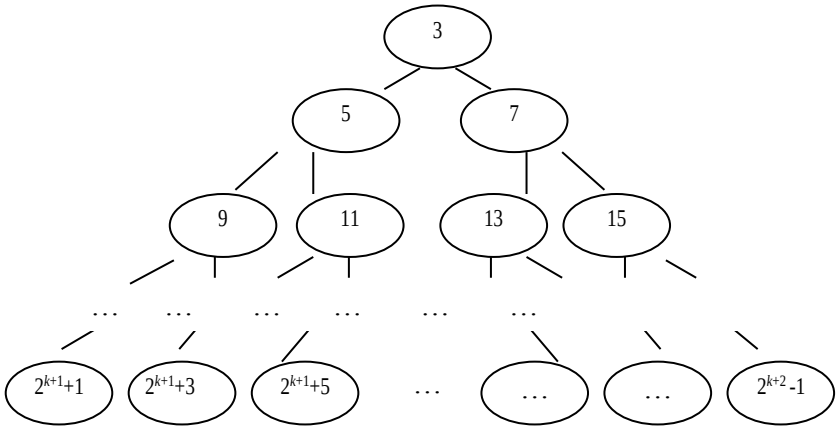


Figure 1. T_3 tree

2.2 Lemmas

Let $N_{(0,0)}$ be an odd number and $T_{N_{(0,0)}}$ be the $N_{(0,0)}$-rooted binary tree. If $N_{(0,0)}=3$, then $T_{N_{(0,0)}}$ becomes T_3. Let $N_{(k,j)}^{N_{(0,0)}}$ be a node in $T_{N_{(0,0)}}$; let $N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}}$ be a node in $T_{N_{(k,j)}^{N_{(0,0)}}}$. Relationships among $N_{(0,0)}$, $T_{N_{(0,0)}}$, $N_{(k,j)}^{N_{(0,0)}}$, $N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}}$ and $T_{N_{(k,j)}^{N_{(0,0)}}}$ are intuitionally depicted by figure 2.

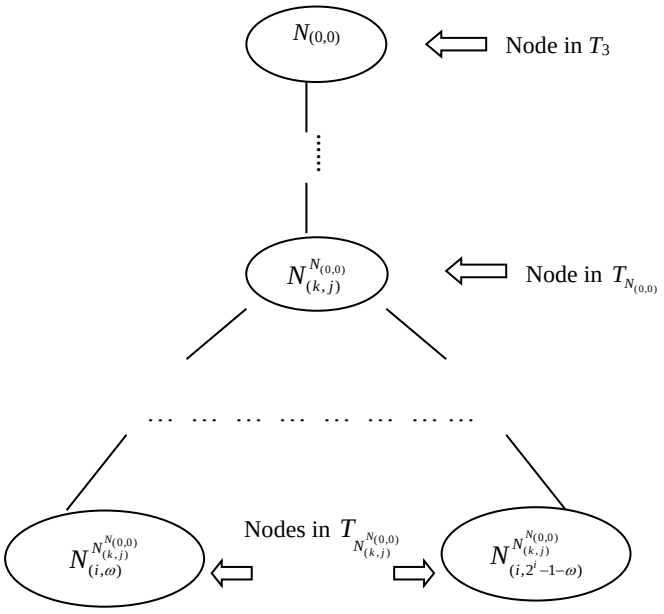


Figure 2. Relationships among nodes of T_3 tree, T_3's subtree and subsubtree.

Articles [1] , [2] and [3] have proven the following Lemmas 1 to 5.

Lemma 1. *For* $T_{N_{(0,0)}}$ *it holds*

(1) There are 2^k *nodes on the* k^{th} *level,* $k=0,1,\ldots$*;*

(2) Node $N_{(k,j)}^{N_{(0,0)}}$ *is computed by*

$$N_{(k,j)}^{N_{(0,0)}}=2^k N_{(0,0)}-2^k+2j+1; k=0,1,2,\ldots; j=0,1,\ldots,2^k-1 \quad (1)$$

(3) Two position-symmetric nodes, $N_{(i,\omega)}^{N_{(0,0)}}$ *and* $N_{(i,2^i-1-\omega)}^{N_{(0,0)}}$*, satisfy*

$$N_{(i,\omega)}^{N_{(0,0)}}+N_{(i,2^i-1-\omega)}^{N_{(0,0)}}=2^{i+1}N_{(0,0)} \quad (2)$$

(4) There is not a multiple of $N_{(0,0)}$ *before the level* $1+\lfloor \log_2 N_{(0,0)} \rfloor$*, there are exactly 2 multiples of* $N_{(0,0)}$ *on the level* $1+\lfloor \log_2 N_{(0,0)} \rfloor$.

Lemma 2. *The i^{th} $(i \geq 0)$ level of subtree $T_{N_{(k,j)}^{N_{(0,0)}}}$ $(k \geq 0)$ is the $(k+i)^{th}$ level of $T_{N_{(0,0)}}$ and it contains 2^i nodes. Node $N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}}$ of $T_{N_{(k,j)}^{N_{(0,0)}}}$ $(0 \leq \omega \leq 2^i - 1)$ is corresponding to node $N_{(k+i,2^i j+\omega)}^{N_{(0,0)}}$ of $T_{N_{(0,0)}}$ by the following formula (3)*

$$N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}} = N_{(k+i,2^i j+\omega)}^{N_{(0,0)}} = 2^i N_{(k,j)}^{N_{(0,0)}} - 2^i + 2\omega + 1;\ j = 0,1,...,2^k - 1; i = 0,1,...; \omega = 0,1,...,2^i - 1 \tag{3}$$

Lemma 3. *Two position-symmetric nodes on each level of $T_{N_{(i,\omega)}^{N_{(0,0)}}}$ fit the following laws*

$$N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(0,0)}}} + N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(0,0)}}} = 2^{i+1} N_{(0,0)}^{N_{(i,\omega)}^{N_{(0,0)}}} \tag{4}$$

or

$$N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(0,0)}}} + N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(0,0)}}} = 2^{i+1} N_{(k,j)}^{N_{(0,0)}} \tag{5}$$

or

$$N_{(k+i,2^i j+\omega)}^{N_{(0,0)}} + N_{(k+i,2^i j+2^i-1-\omega)}^{N_{(0,0)}} = 2^{i+1} N_{(k,j)}^{N_{(0,0)}} \tag{6}$$

where $0 \leq \omega \leq 2^i - 1$.

Lemma 4 (Symmetric Law of Common Divisors) *Suppose node $N_{(k,j)}^{N_{(0,0)}}$ has a common divisor d with $N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}}$, then d is also a common divisor of $N_{(k,j)}^{N_{(0,0)}}$ and $N_{(i,2^i-1-\omega)}^{N_{(k,j)}^{N_{(0,0)}}}$, namely,* $d \mid \gcd(N_{(k,j)}^{N_{(0,0)}}, N_{(i,\omega)}^{N_{(k,j)}^{N_{(0,0)}}}) \Leftrightarrow d \mid \gcd(N_{(k,j)}^{N_{(0,0)}}, N_{(i,2^i-1-\omega)}^{N_{(k,j)}^{N_{(0,0)}}})$.

Lemma 5 *Let p be a positive odd integer; then among p consecutive positive odd integers there exists one and only one that can be divisible by p. Let q be a positive odd number and S be a finite set that is composed of consecutive odd numbers; then S needs at least $(n-1)q+1$ elements to have n multiples of q.*

Lemma 6. *Suppose $N_{(k,j)}$ is a odd number such that $2^{k+1}+1 \leq N_{(k,j)} \leq 2^{k+2}-1$ and $T_{N_{(k,j)}}$ is an $N_{(k,j)}$-rooted valuated binary tree; then there are at least 2^χ multiple-nodes of $N_{(k,j)}$ on level $1+\lfloor \log_2 N_{(k,j)} \rfloor + \chi$ of $T_{N_{(k,j)}}$ for arbitrary integer $\chi > 0$, and all these 2^χ multiple-nodes are subordinate to the symmetric law of common divisors*.

Proof. First, prove the following assertions.

(1) On the $(k+2)^{th}$ level of $T_{N_{(k,j)}}$, there are exact 2 multiple-nodes of $N_{(k,j)}$;

(2) On the $(k+i)^{th}$ level of $T_{N_{(k,j)}}$, there at least 2^{i-2} nodes that are multiple-nodes of $N_{(k,j)}$, where $i \geq 2$;

(3) The multiple-nodes of $N_{(k,j)}$ are symmetrically distributed on each of their existing levels.

In fact, there are 2^{k+i} nodes on the $(k+i)^{th}$ level of $T_{N_{(k,j)}}$. Take the case that $N_{(k,j)} = 2^{k+2} - 1$, namely, $N_{(k,j)}$ takes its maximal value; then owning to

$$2^{k+i} = 2^{i-2}(2^{k+2} - 1) + 2^{i-2}$$

it knows by Lemma 5 that, there are at least 2^{i-2} multiple-nodes on the $(k+i)^{th}$ level of $T_{N_{(k,j)}}$ when $i \geq 2$.

The special case when $i = 2$ yields

$$2^{k+2} = (2^{k+2} - 1) + 1 = N_{(k,j)} + 1$$

which indicates that there is at least 1 multiple-node on the level k+2. And the symmetric law ensures that there are exact 2, which also validates Lemma 1(4) in another way.

Now since $k = \lfloor \log_2 N_{(k,j)} \rfloor - 1$, it yields

$$(k+i)|_{i\geq 2} = (1 + \lfloor \log_2 N_{(k,j)} \rfloor + \chi)|_{\chi \geq 0}$$

This finally validates the lemma.

III. MAIN RESULTS AND PROOFS

Main results include genetic traits of factors' transitions among odd numbers, building of genetic structure, genetic graph and complementary genetic graph, distribution of divisors of an odd composite number, and new criterion of primality test and new approaches to factorize an odd composite number. They are introduced separately in the following sections.

3.1 Genetic Traits of Factors' Transitions

Theorem 1(Genetic Law 1) *If node* $N_{(k,j)}$ *of* T_3 *can divide* $N_{(i,\omega)}^{N_{(k,j)}}$ *of* $T_{N_{(k,j)}}$, *then it can also divide* $N_{(i,2^i-1-\omega)}^{N_{(k,j)}}$ *of* $T_{N_{(k,j)}}$. *And it can also divide nodes* $N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$, $N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$, $N_{(i,\omega)}^{N_{(i,2^i-1-\omega)}^{N_{(k,j)}}}$ *and* $N_{(i,2^i-1-\omega)}^{N_{(i,2^i-1-\omega)}^{N_{(k,j)}}}$ *whose roots are* $N_{(i,\omega)}^{N_{(k,j)}}$ *and* $N_{(i,2^i-1-\omega)}^{N_{(k,j)}}$ *respectively. Namely,* $N_{(k,j)}$ *transmits its genes to its descendents by making itself a divisor of its certain descendents*.

Proof. The conclusion that $N_{(k,j)}$ dividing $N_{(i,\omega)}^{N_{(k,j)}}$ results in its dividing $N_{(i,2^i-1-\omega)}^{N_{(k,j)}}$ can be directly obtained by Lemma 1 to 4. Next is to show $N_{(k,j)} \mid N_{(i,\omega)}^{N_{(k,j)}} \Rightarrow N_{(k,j)} \mid N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$ and $N_{(k,j)} \mid N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$.

In fact, let $\chi = -2^i + 2\omega + 1$; then by Lemma 2 it yields

$$N_{(i,\omega)}^{N_{(k,j)}} = 2^i N_{(k,j)} - 2^i + 2\omega + 1 = 2^i N_{(k,j)} + \chi$$

which says $N_{(k,j)} \mid N_{(i,\omega)}^{N_{(k,j)}} \Rightarrow N_{(k,j)} \mid \chi$.

Then again by Lemma 2 it holds

$$N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}} = 2^i N_{(i,\omega)}^{N_{(k,j)}} + \chi \text{ and } N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}} = 2^i N_{(i,\omega)}^{N_{(k,j)}} - \chi$$

which leads to $N_{(k,j)} \mid N_{(i,\omega)}^{N_{(k,j)}} \Rightarrow N_{(k,j)} \mid N_{(i,\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$ and $N_{(k,j)} \mid N_{(i,2^i-1-\omega)}^{N_{(i,\omega)}^{N_{(k,j)}}}$.

Theorem 2. (Genetic Law 2) *Let odd number $N_{(m,\alpha)}$ be a multiplication of two odd numbers, $N_{(k,j)}$ and $N_{(l,s)}$, namely, $N_{(m,\alpha)} = N_{(k,j)} \times N_{(l,s)}$; then subtree $T_{N_{(m,\alpha)}}$ inherits all genetic traits from both $N_{(k,j)}$ and $N_{(l,s)}$. In another word, if $d_{(i,\omega)}$ is a common divisor of $N_{(k,j)}$ and $N_{(i,\omega)}^{N_{(k,j)}}$, which lies at the ω^{th} position on the i^{th} level in $T_{N_{(k,j)}}$, then $d_{(i,\omega)}$ is also a common divisor of $N_{(m,\alpha)}$ and $N_{(i,\omega)}^{N_{(m,\alpha)}}$.*

Proof. Since $d_{(i,\omega)}$ is a common divisor of $N_{(k,j)}$ and its descendant node $N_{(i,\omega)}^{N_{(k,j)}}$, hence $N_{(k,j)} = d_{(i,\omega)}a$ and $N_{(i,\omega)}^{N_{(k,j)}} = d_{(i,\omega)}b$, where a and b are integers bigger than 1. Consequently $d_{(i,\omega)}$ is of course a divisor of $N_{(m,\alpha)}$ because $N_{(m,\alpha)} = N_{(k,j)} \times N_{(l,s)} = ad_{(i,\omega)} \times N_{(l,s)}$. Next is to show $d_{(i,\omega)} \mid N_{(i,\omega)}^{N_{(m,\alpha)}}$.

Since $N_{(k,j)} = 2^{k+1} + 1 + 2j$ and $N_{(i,\omega)}^{N_{(k,j)}} = N_{(k+i,2^i j+\omega)} = 2^{k+i+1} + 1 + 2^{i+1} j + 2\omega$, it yields

$$d_{(i,\omega)}a = N_{(k,j)} = 2^{k+1} + 1 + 2j,$$

$$d_{(i,\omega)}b = 2^{k+i+1} + 1 + 2^{i+1} j + 2\omega.$$

Rewrite $d_{(i,\omega)}b$ by

$$d_{(i,\omega)}b = 2^{k+i+1} + 1 + 2^{i+1} j + 2\omega - 2^i + 2^i$$

and let $\chi = 2\omega + 1 - 2^i$; then it holds

$$d_{(i,\omega)}b = 2^{k+i+1} + 2^{i+1} j + 2^i + \chi = 2^i N_{(k,j)} + \chi = 2^i d_{(i,\omega)}a + \chi$$

Hence

$$\chi = d_{(i,\omega)}(b - 2^i a)$$

Consequently it yields

$$\begin{aligned} N_{(i,\omega)}^{N_{(m,\alpha)}} &= 2^i N_{(m,\alpha)} - 2^i + 2\omega + 1 = 2^i N_{(m,\alpha)} + \chi \\ &= 2^i N_{(k,j)} \times N_{(l,s)} + d_{(i,\omega)}(b - 2^i a) \\ &= d_{(i,\omega)}(2^i a N_{(l,s)} + b - 2^i a) \end{aligned}$$

which says $d_{(i,\omega)}$ is a common divisor of $N_{(m,\alpha)}$ and $N_{(i,\omega)}^{N_{(m,\alpha)}}$.

Theorem 1 can be intuitionally depicted by figure 3. Figures 4 and 5 are two examples of Theorem 1, figure 6 is an example of Theorem 2.

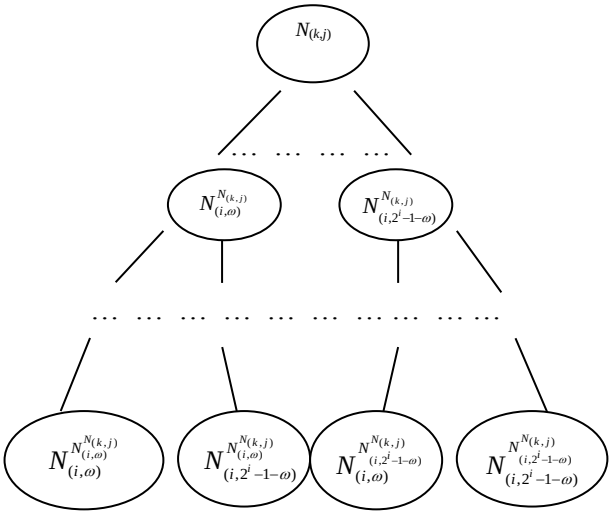


Figure 3. Gene Transitions between root and its descendents

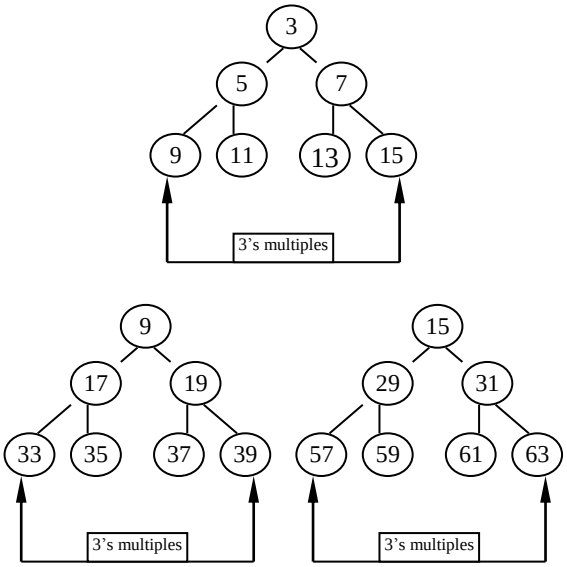


Figure 4. 9 and 15 inherit 3's genes and descend them to their own descendents as 3 does

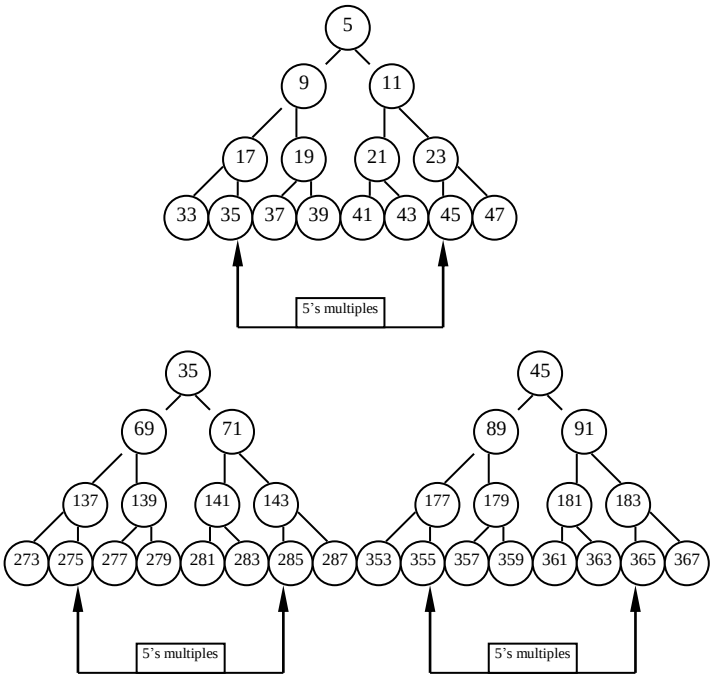


Figure 5. 35 and 45 inherit 5's genes and descend them to their own descendents as 5 does

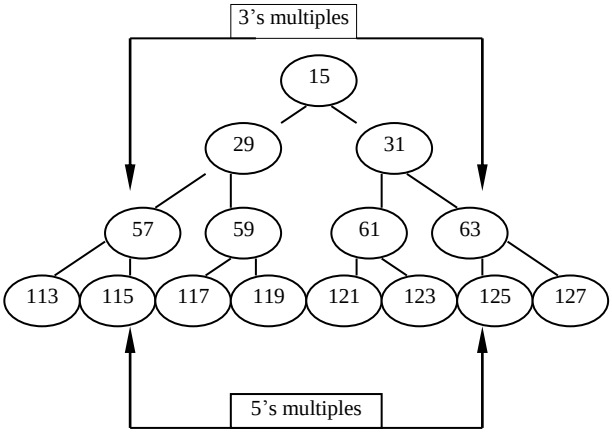


Figure 6. 15 inherits genetic traits from both 3's and 5's

3.2 Genetic Graph of Prime Number *p*

Let $p>2$ be a prime number and T_p be the p-rooted valuated binary tree; then according to Theorems 1 and 2, p transmits its genes to its descendents, which are actually nodes of T_p. It can see that such heredity process is highly related with the logical structure of the root p and its two nearest multiples in T_p as claimed in Lemma 1(4). This section investigates such structure and the role it plays in the heredity process in T_p.

Definition 2 Let $p>2$ be a prime number and T_p be the p-rooted valuated binary tree; then the geometric structure formed by the root p and its two multiples on the level $1+\lfloor \log_2 p \rfloor$ of T_p together with the paths from p to the two multiples is called genetic structure of p, as illustrated in figure 7. p's genetic structure is denoted by symbol $g(p)$ and its five elements are denoted by $g^p_{(0,0)}, g^p_{(1,0)}$, $g^p_{(1,1)}$, $e^p_{(0,0)}$ and $e^p_{(0,1)}$, respectively.

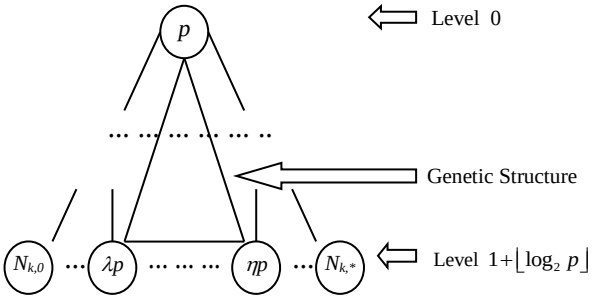


Figure 7. Genetic Structure

Comments. Since there is a unique path connecting the root *p* and each of its sons, paths are usually expressed with simple straight lines and their concrete geometric shapes are ignored unless special demands.

Definition 3. Let *p*>2 be a prime number and T_p be the *p*-rooted valuated binary tree; then *p*'s genetic graph *G*(*p*) is T_p's subtree that is recursively generated by the following rules.

1. *G*(*p*) is rooted by *p*;
2. Each node *n* of *G*(*p*) has two suns, a left son and a right son; the father and the two sons as well as the two paths connecting the father and the two sons respectively form a genetic structure $g(n)$;
3. Two different nodes n_1 and n_2 satisfy $g(n_1) \cap g(n_2) = \varnothing$; and $g(n_1) = g(n_2)$ if and only if $n_1 = n_2$;
4. $G(p) = \bigcup_{n=p}^{\infty} g(n)$.

Then by Definition 3, Lemma 1(4) and Lemma 2, the following Theorem 3 and Theorem 4 hold.

Theorem 3. *Let p>2 be a prime number and* T_p *be the p-rooted valuated binary tree; then p's genetic structure consists of three nodes and two paths of* T_p *by*

(i) $g^p_{(0,0)} = N_{(0,0)} = p$;

(ii) $g_{(1,0)} = N^{N_{(0,0)}}_{(k,s)}, g_{(1,1)} = N^{N_{(0,0)}}_{(k,t)}$, *where* $k = 1 + \lfloor \log_2 p \rfloor, s = \left\lfloor (2^{1+\lfloor \log_2 p \rfloor} - p - 1)/2 \right\rfloor, t = \left\lfloor (2^{1+\lfloor \log_2 p \rfloor} + p - 1)/2 \right\rfloor$

(iii) *path* $e^p_{(0,0)}$ *connects p and* $g^p_{(1,0)}$, *and* $e^p_{(0,1)}$ *connects p and* $g_{(1,1)}$.

Theorem 4. *Let p>2 be a prime number and* T_p *be the p-rooted valuated binary tree; then p's genetic graph G(p) is a complete full binary tree and can be recursively constructed.*

3.3 Complementary Genetic Graph of Prime Number *p*

It knows from Definition 3 that, each node of *G*(*p*) is a multiple of *p*. Since there exist *p*'s other multiple-nodes in T_p, it is mandatory to define the following complementary genetic graph to describe these nodes.

Definition 4. Let $p>2$ be a prime number and T_p be the p-rooted valuated binary tree; then p's complementary genetic graph $G^*(p)$ is a binary tree that is subordinate to the following rules.

(1) Nodes and edges of $G^*(p)$ come from T_p and $G^*(p)$ is rooted by p;

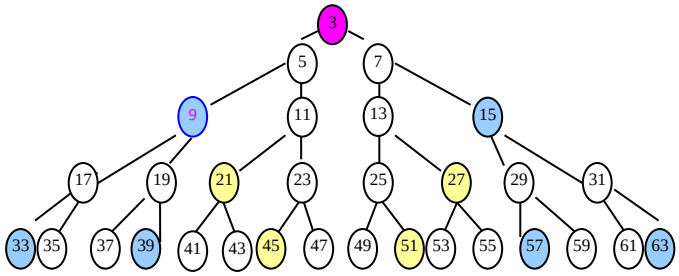
(2) Each node of $G^*(p)$ is a multiplication of p and an odd number bigger than 1;

(3) Arbitrary node $n \in G^*(p)$ such that $n \neq p$ satisfies $n \notin G(p)$, that is, $G(p) \cap G^*(p) = p$.

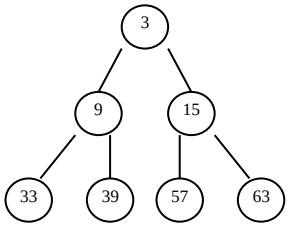
Then by Lemma 4, the following Theorem 5 holds.

Theorem 5. *Let $p>2$ be a prime number and T_p be the p-rooted valuated binary tree; then $G^*(p)$ is a symmetric binary tree, that is, its left subtree and right subtree are subordinate to symmetric laws of position and common divisors*.

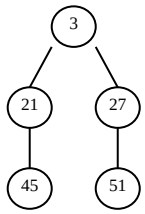
Figure 8 shows the T_3 tree, 3's genetic graph and its complementary genetic graph.



(*a*) T_3 tree



(*b*) 3's genetic graph



(*c*) 3's complementary genetic graph

Figure 8. T_3 tree, 3's genetic graph and its complementary genetic graph

Obviously, by definitions of $G(p)$ and $G^*(p)$, the following Theorem 6 holds.

Theorem 6. *Suppose p is an odd prime number and* T_p *is the p-rooted valuated binary tree; let* k_g *be the level of* T_p *where level 1 of G(p) occurs and* k_g^* *be the level of* T_p *where level 1 of* $G^*(p)$ *occurs; then* $k_g^* \geq k_g + 1$.

3.4 Genetic Laws of Factors' Transition in Odd Composite Numbers

Theorem 7. *Suppose* $3 \leq p < q$ *are odd numbers bigger and* $N_{(m,\alpha)} = pq$ *; let* $k_q = 1 + \lfloor \log_2 q \rfloor$ *and* $s = \left\lfloor (2^{1+\lfloor \log_2 q \rfloor} - q - 1)/2 \right\rfloor, t = \left\lfloor (2^{1+\lfloor \log_2 q \rfloor} + q - 1)/2 \right\rfloor$ *; then there are at least 2 multiple-nodes of p that are symmetrically distributed between* $N_{(k_q,s)}^{N_{(m,\alpha)}}$ *and* $N_{(k_q,t)}^{N_{(m,\alpha)}}$.

Proof. Let $\delta = t - s$; then by properties of the floor function, see in [4] and [5], it yields

$$t - s = \left\lfloor (2^{1+\lfloor \log_2 q \rfloor} + q - 1)/2 \right\rfloor - \left\lfloor (2^{1+\lfloor \log_2 q \rfloor} - q - 1)/2 \right\rfloor \geq \left\lfloor (2^{1+\lfloor \log_2 q \rfloor} + q - 1)/2 - (2^{1+\lfloor \log_2 q \rfloor} - q - 1)/2 \right\rfloor = q$$

which says that there are at least q nodes between $N_{(k_q,s)}^{N_{(m,\alpha)}}$ and $N_{(k_q,t)}^{N_{(m,\alpha)}}$. Since $p<q$, it knows there must exist at least one p's multiple-node between $N_{(k_q,s)}^{N_{(m,\alpha)}}$ and $N_{(k_q,t)}^{N_{(m,\alpha)}}$. By symmetric law, the theorem holds.

Theorem 8. *Suppose* $2^{m+1} + 1 \leq N_{(m,\alpha)} \leq 2^{m+2} - 1$ *is an odd number and* $N_{(m,\alpha)} = pq$ *, where m>0 is an integer,* $3 \leq p < q$ *are odd coprimed numbers; let* $\vartheta = \lfloor \log_2 N_{(m,\alpha)} \rfloor$*; then there must be at least two p's multiple-nodes and two q's multiple-nodes on level* ϑ *of* $T_{N_{(m,\alpha)}}$. *All the multiple-nodes of p and q are subordinate to the symmetric law and the p's multiple-nodes are distinct from the q's multiple-nodes.*

Proof. The assumption that $m>0$ and $2^{m+1} + 1 \leq N_{(m,\alpha)} \leq 2^{m+2} - 1$ yields

$$2^{\frac{m+1}{2}} < \sqrt{2^{m+1} + 1} \leq \sqrt{N_{(m,\alpha)}} \leq \sqrt{2^{m+2} - 1} < 2^{\frac{1}{2} + \frac{m+1}{2}} \tag{7}$$

Since $m = \lfloor N_{(m,\alpha)} \rfloor - 1$, it knows $m + 2 = 1 + \lfloor N_{(m,\alpha)} \rfloor$ and thus $\vartheta = m + 1$. Because there are 2^{m+1} nodes on the level ϑ of $T_{N_{(m,\alpha)}}$ and $2^{m+1} > 2^{\frac{1}{2} + \frac{m+1}{2}} > \sqrt{N_{(m,\alpha)}}$ for arbitrary $m > 0$, it knows by Lemma 5 that there are at least two p's multiple nodes that are symmetrically distributed on the level ϑ. On the other hand, $N_{(m,\alpha)} = pq$ and $q > p \geq 3$ yield $N_{(m,\alpha)} \geq 3q$, namely,

$$q \le \frac{N_{(m,\alpha)}}{3} \le \frac{2^{m+2}-1}{3} < 2^{m+1} \tag{8}$$

Hence there are at least two *q*'s multiple-nodes that are symmetrically distributed on the level ϑ. By symmetric law, it is obvious that all the *p*'s and *q*'s multiple-nodes are symmetrically distributed. Next is to prove that the *p*'s multiple-nodes are distinct from the *q*'s multiple-nodes if *p* and *q* are coprimed. In fact, if a *p*'s multiple-node is also a *q*'s multiple-node, or vice versa, then it must be a multiple-node of $pq = N_{(m,\alpha)}$ due to the coprimality of *p* to *q*. This is contrast to the fact that $N_{(m,\alpha)}$ has no multiple-nodes before level $1+\lfloor N_{(m,\alpha)} \rfloor$ according to Lemma 1(4). Hence the theorem holds.

Corollary 1. *If p>2 is an odd number and* $N_{(m,\alpha)} = p^2$*, then there are exactly least two p's multiple-nodes that are symmetrically distributed on level* $\lfloor \log_2 N_{(m,\alpha)} \rfloor$ *of* $T_{N_{(m,\alpha)}}$.

Theorem 9. *Suppose* $2^{m+1}+1 \le N_{(m,\alpha)} \le 2^{m+2}-1$ *is an odd number and* $N_{(m,\alpha)} = pq$*, where m>1 is an integer,* $3 \le p \le q$ *are odd coprime numbers; let* $\sigma = \lfloor \log_2 N_{(m,\alpha)} \rfloor - 1$*; then there must be at least two p's multiple-nodes that are symmetrically distributed on level* σ *of* $T_{N_{(m,\alpha)}}$.

Proof. Since $\sigma = \lfloor \log_2 N_{(m,\alpha)} \rfloor - 1 = m$, there are $2^m = 2^\sigma$ nodes on level σ. The inequality $3 \le p \le q$ yields $3 \le p \le \sqrt{N_{(m,\alpha)}} \le q$. Hence $p < 2^{\frac{1}{2}+\frac{m+1}{2}}$. Referring to inequality (7) yields $\frac{p}{2^m} < \frac{\sqrt{N_{(m,\alpha)}}}{2^m} < \frac{2^{\frac{1}{2}+\frac{m+1}{2}}}{2^m} = 2^{1-\frac{m}{2}}$, and it knows that $p < 2^m$ when *m*>1. Hence on the level σ, there is at least one *p*'s multiple-node. By the symmetric law the level σ contains at least 2 *p*'s multiple-nodes.

3.5 New Criterion of Primality and Factorization of Integers

Theorem 10. *Let* $N_{(m,\alpha)} > 1$ *be an odd number and* $T_{N_{(m,\alpha)}}$ *be the* $N_{(m,\alpha)}$*-rooted valuated binary tree. If* $N_{(m,\alpha)}$ *has no common divisor with any node from level 1 to level* $\lfloor \log_2 N_{(m,\alpha)} \rfloor$ *of* $T_{N_{(m,\alpha)}}$*, then* $N_{(m,\alpha)}$ *is a prime number*.

Proof. Use proof by contradiction. Assume $N_{(m,\alpha)} = N_{(k,j)} \times N_{(l,s)}$ to be a composite number; then $k < m$ and $l < m$. By Lemma 1(4) and Theorem 2, either $N_{(k,j)}$ or $N_{(l,s)}$ has a divisor after level 1 and before level $1+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ of $T_{N_{(m,\alpha)}}$, which is contradict to the condition of the theorem. Hence the theorem holds.

Theorem 11. *Let* $n \geq 2$ *and* $N_{(m,\alpha)} = p_1 p_2 ... p_n$, *where* $p_1, p_2, ..., p_n$ *are odd numbers bigger than 1; then the bigger n is, the easier* $N_{(m,\alpha)}$ *is factorized. If* $n = 2$ *and* $p_1 < p_2$; *then the bigger* $\kappa = \frac{p_2}{p_1}$ *is, the easier* $N_{(m,\alpha)}$ *is factorized.*

Proof. Let $K = 1 + \lfloor \log_2 N_{(m,\alpha)} \rfloor$, $s = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} - N_{(m,\alpha)} - 1)/2 \right\rfloor$, $t = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} + N_{(m,\alpha)} - 1)/2 \right\rfloor$ and $k_i = 1 + \lfloor \log_2 p_i \rfloor \quad (i = 1,2,...,n)$; then by Lemma 6 there are respectively at least 2^{K-k_i} multiple-nodes of p_i on level *K* of $T_{N_{(m,\alpha)}}$. By Theorem 7, there must exist multiple-nodes of p_i in the interval $[N_{(K,s)}^{N_{(m,\alpha)}}, N_{(K,t)}^{N_{(m,\alpha)}}]$ that contains $N_{(m,\alpha)} + 1$ nodes of $T_{N_{(m,\alpha)}}$. Consequently, the bigger *n* is, the more multiple-nodes are contained in the interval, and thus the easier $N_{(m,\alpha)}$ is factorized because each of the multiple-nodes has a common divisor with $N_{(m,\alpha)}$.

Now consider the case *n*=2. By Lemma 6, there are respectively at least 2^{K-k_1} and 2^{K-k_2} multiple-nodes of p_1 and p_2 on level *K* of $T_{N_{(m,\alpha)}}$. Note that, by Lemma 1, the two nodes on level *K*, $N_{(K,s)}^{N_{(m,\alpha)}}$ and $N_{(K,t)}^{N_{(m,\alpha)}}$, are the only 2 ones that are multiples of both p_1 and p_2. Hence there are totally at least $2 + 2^{K-k_1} + 2^{K-k_2}$ multiple-nodes of p_1 or p_2 on level *K* of $T_{N_{(m,\alpha)}}$.

Let $T(K,k_1,k_2) = 2 + 2^{K-k_1} + 2^{K-k_2}$; then it yields

$$T(K,k_1,k_2) = 2 + 2^{K-k_2}(2^{k_2-k_1} + 1)$$

Since $K - k_2 = \lfloor \log_2 p_1 p_2 \rfloor - \lfloor \log_2 p_2 \rfloor \geq \lfloor \log_2 p_1 p_2 - \log_2 p_2 \rfloor = \lfloor \log_2 p_1 \rfloor$ and $k_2 - k_1 = \lfloor \log_2 p_2 \rfloor - \lfloor \log_2 p_1 \rfloor \geq \left\lfloor \log_2 \frac{p_2}{p_1} \right\rfloor$, it results in

$$T(K,k_1,k_2) \geq 2 + \lfloor \log_2 p_1 \rfloor \left(\left\lfloor \log_2 \frac{p_2}{p_1} \right\rfloor + 1 \right) \tag{9}$$

Therefore, the bigger $\kappa = \frac{p_2}{p_1}$ is, the more multiples lie on level *K*, and thus the easier $N_{(m,\alpha)}$ is factorized.

Theorem 12. *Suppose* $N_{(m,\alpha)}$ *is an odd composite number that fits* $2^{m+1} + 1 \leq N_{(m,\alpha)} \leq 2^{m+2} - 1$ *and* $N_{(m,\alpha)} = pq$ *such that p and q are odd numbers such that* $3 \leq p \leq q$; *let* $K = 1 + \lfloor \log_2 N_{(m,\alpha)} \rfloor = m + 2$, $s = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} - N_{(m,\alpha)} - 1)/2 \right\rfloor$, $t = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} + N_{(m,\alpha)} - 1)/2 \right\rfloor$; *use symbols* $N_{(K,\omega(q))}^{N_{(m,\alpha)}}$ *and* $N_{(K,\omega(p))}^{N_{(m,\alpha)}}$ *respectively to indicate the first q's and the first p's multiple-nodes that are left to the node* $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$; *then there*

are exactly $\frac{N_{(m,\alpha)}+1}{2}$ *nodes from* $N_{(K,s)}^{N_{(m,\alpha)}}$ *to* $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$, *there are at least* $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ *and at most* 2^m *nodes from* $N_{(K,\omega(q))}^{N_{(m,\alpha)}}$ *to* $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$, *and there are at most* $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ *nodes from* $N_{(K,\omega(p))}^{N_{(m,\alpha)}}$ *to* $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$, *as illustrated by figure 9, where the symbol Con means "counts of nodes".*

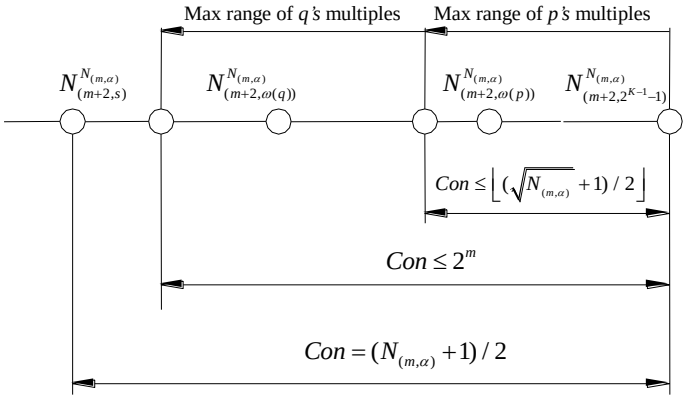


Figure 9. Divisors' distribution

Proof. The first conclusion that there are exactly $\frac{N_{(m,\alpha)}+1}{2}$ nodes from $N_{(K,s)}^{N_{(m,\alpha)}}$ to $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$ can be directly drawn from Lemma 5. Next is to prove the other ones. Since $N_{(m,\alpha)} = pq$ and $3 \le p \le q$, it yields $p \le \sqrt{N_{(m,\alpha)}}$ and $q \ge \sqrt{N_{(m,\alpha)}}$. Referring to the proof of Theorem 11, it knows that, when $K = 1 + \lfloor \log_2 N_{(m,\alpha)} \rfloor$, $s = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} - N_{(m,\alpha)} - 1)/2 \right\rfloor$ and $t = \left\lfloor (2^{1+\lfloor \log_2 N_{(m,\alpha)} \rfloor} + N_{(m,\alpha)} - 1)/2 \right\rfloor$, there must exist p's and q's multiple-nodes that are symmetrically distributed in interval $(N_{(K,s)}^{N_{(m,\alpha)}}, N_{(K,t)}^{N_{(m,\alpha)}})$ on level K of $T_{N_{(m,\alpha)}}$. Let $N_{(K,q_1)}^{N_{(m,\alpha)}}$ and $N_{(K,q_2)}^{N_{(m,\alpha)}}$ be the two neighboring symmetric multiple-nodes of q; then there are q+1 nodes between the two. Since $q \ge \sqrt{N_{(m,\alpha)}}$ it yields

$$\frac{q+1}{2} \ge \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \ge \left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$$

which says that there are at least $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ nodes from $N_{(K,\omega(q))}^{N_{(m,\alpha)}}$ to the node $N_{(K,2^{K-1}-1)}^{N_{(m,\alpha)}}$.

On the other hand, referring to (8) yields $\frac{q+1}{2} < \frac{2^{m+1}+1}{2} = 2^m + \frac{1}{2} < 2^m + 1$. Since $\frac{q+1}{2}$ and 2^m+1 are both positive integers, it yields

$$\frac{q+1}{2} \le 2^m \tag{10}$$

which says there are at most 2^m nodes from $N^{N_{(m,\alpha)}}_{(K,\omega(q))}$ to $N^{N_{(m,\alpha)}}_{(K,2^{K-1}-1)}$.

Similarly, let $N^{N_{(m,\alpha)}}_{(K,p_1)}$ and $N^{N_{(m,\alpha)}}_{(K,p_2)}$ be the p's two neighboring symmetric multiple-nodes; then the inequality $p \le \sqrt{N_{(m,\alpha)}}$ results in

$$\frac{p+1}{2} \le \frac{\sqrt{N_{(m,\alpha)}}+1}{2} < \left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor + 1$$

Since $\frac{p+1}{2}$ and $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor + 1$ are integers, it yields

$$\frac{p+1}{2} \le \left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor \tag{11}$$

which says there are at most $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ nodes from $N^{N_{(m,\alpha)}}_{(K,\omega(p))}$ to the node $N^{N_{(m,\alpha)}}_{(K,2^{K-1}-1)}$.

Theorem 13. *Let $N_{(m,\alpha)} = pq$ be an odd composite number such that $2^{m+1}+1 \le N_{(m,\alpha)} \le 2^{m+2}-1$ and $m > 2$, where p and q are odd coprime numbers that fit $3 \le p < q$; let symbols $N^{N_{(m,\alpha)}}_{(m+1,0)}$ and $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ be respectively the leftmost and the rightmost nodes on level m+1 in the left branch of $T_{N_{(m,\alpha)}}$; let $N^{N_{(m,\alpha)}}_{(m+1,\omega(q))}$ and $N^{N_{(m,\alpha)}}_{(m+1,\omega(p))}$ indicate respectively the first q's and p's multiple-nodes left to $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$, $N^{N_{(m,\alpha)}}_{(m+1,\xi(qp))}$ be the node that is left to and $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ nodes away from $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$, and $N^{N_{(m,\alpha)}}_{(m+1,2^{m-1}-1)}$ be the mid-node that is right to and 2^{m-1} nodes away from $N^{N_{(m,\alpha)}}_{(m+1,0)}$; then the distribution of $N^{N_{(m,\alpha)}}_{(m+1,0)}$, $N^{N_{(m,\alpha)}}_{(m+1,\omega(q))}$, $N^{N_{(m,\alpha)}}_{(m+1,2^{m-1}-1)}$, $N^{N_{(m,\alpha)}}_{(m+1,\xi(qp))}$, $N^{N_{(m,\alpha)}}_{(m+1,\omega(p))}$ and $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ on level m+1 is as figure 10 illustrates.*

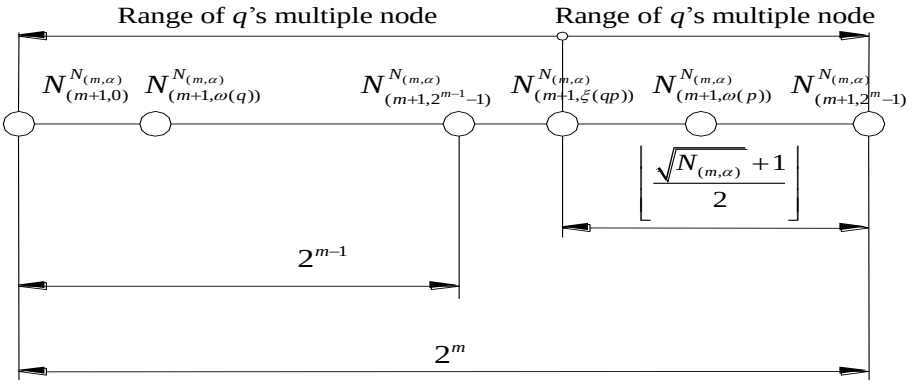


Figure 10. Distribution of Critical Nodes (m>2)

Proof. For convenience, denote the number $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ by $\Xi(N_{(m,\alpha)})$. Then by Theorem 12, it requires at most $\Xi(N_{(m,\alpha)})$ nodes and at most 2^m nodes to find a p's and a q's multiple-node from the rightmost node on a level in the left branch of $T_{N_{(m,\alpha)}}$. Therefore, the node $N^{N_{(m,\alpha)}}_{(m+1,\xi(qp))}$ is actually a boundary-point that stops searching a p's multiple-node from $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ and starts searching a q's multiple-node towards $N^{N_{(m,\alpha)}}_{(m+1,0)}$.

Since

$$2^{\frac{m}{2}-\frac{1}{2}}-\frac{1}{2}<\frac{\sqrt{2^{m+1}+1}+1}{2}-1\le\Xi(N_{(m,\alpha)})\le\frac{\sqrt{N_{(m,\alpha)}}+1}{2}\le\frac{\sqrt{2^{m+2}-1}+1}{2}<2^{\frac{m}{2}}+\frac{1}{2} \tag{12}$$

it yields when m>2

$$\frac{2^{\frac{m}{2}}+\frac{1}{2}}{2^m}=2^{-\frac{m}{2}}+2^{-(m+1)}<1$$

Hence the number of nodes from $N^{N_{(m,\alpha)}}_{(m+1,\xi(pq))}$ to $N^{N_{(m,\alpha)}}_{(m+1,2^m-1)}$ can never exceed the number of nodes in the left branch on level m+1 of $T_{N_{(m,\alpha)}}$ because the later contains 2^m nodes. By Theorem 8, on level $m+1=\lfloor \log_2 N_{(m,\alpha)} \rfloor$ there are at least 4 nodes that have common divisors with $N_{(m,\alpha)}$. It knows by the symmetric law that, among 2^m nodes on level $m+1$in the left branch of $T_{N_{(m,\alpha)}}$, there are at least 2 nodes that have common divisors with $N_{(m,\alpha)}$. By Theorem 12, the two nodes, $N^{N_{(m,\alpha)}}_{(m+1,\omega(q))}$ and $N^{N_{(m,\alpha)}}_{(m+1,\omega(p))}$, do exist and they are respectively left to and right to $N^{N_{(m,\alpha)}}_{(m+1,\xi(qp))}$.

Now investigate the relationship between the mid-node $N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}}$ and the boundary-node $N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}$.

A direct calculation shows

$$\frac{\sqrt{2}}{2^{\frac{m}{2}}}-\frac{1}{2^m}<\frac{\Xi(N_{(m,\alpha)})}{2^{m-1}}<\frac{2}{2^{\frac{m}{2}}}+\frac{1}{2^m}$$

and

$$\frac{\frac{\sqrt{2}}{2^{\frac{m}{2}}}-\frac{1}{2^m}}{\frac{2}{2^{\frac{m}{2}}}+\frac{1}{2^m}}<\frac{\sqrt{2}}{2}$$

These two inequalities indicate the following two conclusions.

(1) When $m>2$, it always holds $0<\frac{\Xi(N_{(m,\alpha)})}{2^{m-1}}<1$, which means that $N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}$ is right to the mid-node $N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}}$, or it holds

$$N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}\in[N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}},N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}]$$

(2) The mid-node $N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}}$ is quite close to $N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}$.

Now it is up to investigating the amounts of nodes in two intervals $[N_{(m+1,0)}^{N_{(m,\alpha)}},N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}]$ and $[N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}},N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}]$.

Note that

$$\frac{2^m-\Xi(N_{(m,\alpha)})}{\Xi(N_{(m,\alpha)})}>\frac{2^m-(2^{\frac{m}{2}}+\frac{1}{2})}{2^{\frac{m}{2}}+\frac{1}{2}}=\frac{2^{m+1}}{2^{\frac{m}{2}+1}+1}-1$$

Since $2^{m+1}-2^{\frac{m}{2}+1}-1=2\times2^{\frac{m}{2}}(2^{\frac{m}{2}}-1)-1>2$ when $m>1$, it knows that the number of nodes in the interval $[N_{(m+1,0)}^{N_{(m,\alpha)}},N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}]$ is bigger than that in the interval $[N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}},N_{(m+1,2^m-1)}^{N_{(m,\alpha)}}]$.

Meanwhile, it can see that, when m>2 it holds

$$\frac{2^m-\Xi(N_{(m,\alpha)})}{2^{m-1}}>\frac{2^m-(2^{\frac{m}{2}}+\frac{1}{2})}{2^{m-1}}=2-2^{1-\frac{m}{2}}-2^{-m}>1$$

which means $N_{(m+1,2^{m-1}-1)}^{N_{(m,\alpha)}}\in[N_{(m+1,0)}^{N_{(m,\alpha)}},N_{(m+1,\xi(qp))}^{N_{(m,\alpha)}}]$ when m>2.

Summarizing all the cases discussed above, it is sure the theorem holds.

Theorem 14. *Let* $N_{(m,\alpha)} = pq$ *be an odd composite number such that* $2^{m+1}+1 \le N_{(m,\alpha)} \le 2^{m+2}-1$ *and* $m > 2$*, where p and q are odd numbers that fit* $3 \le p \le q$*; let symbols* $N_{(m,0)}^{N_{(m,\alpha)}}$, $N_{(m,2^{m-2}-1)}^{N_{(m,\alpha)}}$ *and* $N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}$ *be respectively the leftmost, the middle and the rightmost nodes on level m in the left branch of* $T_{N_{(m,\alpha)}}$*; let* $N_{(m,\omega(p))}^{N_{(m,\alpha)}}$ *indicate the first p's multiple-node left to* $N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}$*; then* $N_{(m,\omega(p))}^{N_{(m,\alpha)}}$ *is at most* $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ *nodes away from* $N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}$*, and it holds that* $N_{(m,\omega(p))}^{N_{(m,\alpha)}} \in [N_{(m,0)}^{N_{(m,\alpha)}}, N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}]$ *if* $2 < m \le 4$ *and* $N_{(m,\omega(p))}^{N_{(m,\alpha)}} \in [N_{(m,2^{m-2}-1)}^{N_{(m,\alpha)}}, N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}]$ *if* $m \ge 5$.

Proof. Referring to (12), it yields when $m \ge 5$

$$\frac{2^{\frac{m}{2}-\frac{1}{2}}-\frac{1}{2}}{2^{m-2}} < \frac{\Xi(N_{(m,\alpha)})}{2^{m-2}} < \frac{2^{\frac{m}{2}}+\frac{1}{2}}{2^{m-2}} \Rightarrow 0 < 2^{-\frac{m}{2}+\frac{3}{2}} - 2^{-m+1} < \frac{\Xi(N_{(m,\alpha)})}{2^{m-2}} < 2^{-\frac{m}{2}+2} + 2^{-m+1} < 1$$

which says $N_{(m,\omega(p))}^{N_{(m,\alpha)}} \in [N_{(m,2^{m-2}-1)}^{N_{(m,\alpha)}}, N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}]$ if $m \ge 5$.

The rest of the proof can refer to the proof of Theorem 13.

Corollary 2. *Let* $N_{(m,\alpha)}$ *be an odd composite number; then it requires at most* $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ *searching steps to find a divisor of* $N_{(m,\alpha)}$.

Corollary 3. *Let* $2^{m+1}+1 \le N_{(m,\alpha)} \le 2^{m+2}-1$ *and* $k = \lfloor \log_2 N_{(m,\alpha)} \rfloor - 1$ *with* $m > 4$*; then* $N_{(m,\alpha)}$ *is a prime number if it has no divisor in* $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ *consecutive nodes left to* $N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}$.

Proof. By Theorem 14 and Corollary 2, the assumption that $N_{(m,\alpha)}$ has no divisor in $\left\lfloor \frac{\sqrt{N_{(m,\alpha)}}+1}{2} \right\rfloor$ consecutive nodes left to $N_{(m,2^{m-1}-1)}^{N_{(m,\alpha)}}$ means that it has no divisor that is less than $\sqrt{N_{(m,\alpha)}}$, which means $N_{(m,\alpha)}$ is prime.

Corollary 4. *Let* $N_{(m,\alpha)}$ *be an odd composite number; then there exist approaches that find a divisor of* $N_{(m,\alpha)}$ *in no more than* $2+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ *searches.*

Proof. By genetic law, a divisor *d* of $N_{(m,\alpha)}$ lies either on $N_{(m,\alpha)}$'s genetic structure or on its complementary genetic structure. If *d* is on $N_{(m,\alpha)}$'s genetic structure, by Theorem 7

it takes at most $1+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ steps to reach the level $1+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ along certain path from $N_{(m,\alpha)}$ to the node that has *d* as a divisor. If *d* is on $N_{(m,\alpha)}$'s complementary genetic structure, it takes at most $2+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ steps to the level after the level $1+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ because the level $2+\lfloor \log_2 N_{(m,\alpha)} \rfloor$ surely contains nodes that have *d* as their divisors by Lemma 6.

4. ALGORITHM DESIGN AND NUMERICAL EXPERIMENTS

Algorithms to factorize odd composite numbers can be designed according to the previous theorems. This section presents two basic algorithms. One is a sequential searching (SS) approach based on Theorem 14, the other is a subdivision and squeeze searching (SSS) approach.

4.1 Sequential Searching Algorithm

Sequential searching algorithm searches a node of *p*'s multiples that contain common divisors with the root, which can reach *O*(1) in the best case and $\frac{1}{2}\sqrt{N_{(0,0)}}$ in the worst case. The algorithm is as follows.

======== Sequential Searching Algorithm==========

Input: Odd composite number $N_{(0,0)}$

Step 1. Calculate searching level: $K=\lfloor \log_2 N_{(0,0)} \rfloor -1$;

Step 2. Calculate the largest searching steps: $l_{\max}=\left\lfloor (\sqrt{N_{(0,0)}}+1)/2 \right\rfloor$;

Step 3. Calculate lower and upper limits: $ul=N^{N_{(0,0)}}_{(K,2^{K-1}-1)}, ll=ul-2l_{\max}$;

Step 4. Search in interval $[ll,ul]$ the first odd number that has common divisor with $N_{(0,0)}$.

==========End of Algorithm ==========

4.2 Subdivision & Squeeze Searching Algorithm

The sequential searching algorithm searches every possible node from $ul=N^{N_{(0,0)}}_{(K,2^{K-1}-1)}$ to $ll=ul-2l_{\max}$. According to Theorem 11 it will cost a lot of time when an odd composite number contains only two factors that are very close to one another. Using

subdivision and squeeze search approach can decrease the searching steps.

====== Subdivision Squeeze Searching Algorithm=======

Input: Odd composite number $N_{(0,0)}$, subdivision ratio ζ.

Step 1. Calculate searching level: $K = \lfloor \log_2 N_{(0,0)} \rfloor - 1$;

Step 2. Calculate the largest searching steps: $l_{\max} = \lfloor (\sqrt{N_{(0,0)}} + 1)/2 \rfloor$;

Step 3. Calculate variables:

$$ul = N_{(K,2^{K-1}-1)}^{N_{(0,0)}}; ll = ul - 2l_{\max};$$

$$ml = ll + \zeta l_{\max}; left = ml - 2; right = ml + 2$$

Step 4. If *FindGCD*($N_{(0,0)}$,*ll*) or *FindGCD*($N_{(0,0)}$,*ul*)

or *FindGCD*($N_{(0,0)}$,*ml*) return *GCD*;

Else

Begin loop

$ul = ul - 2; ll = ll + 2; left = left - 2; right = right + 2$

If *FindGCD*($N_{(0,0)}$,*ll*) or *FindGCD*($N_{(0,0)}$,*ul*)

or *FindGCD*($N_{(0,0)}$,left) or *FindGCD*($N_{(0,0)}$,*right*)

return *GCD*;

End loop

==========End of Algorithm ==========

Comments. The subdivision and squeeze searching algorithm can vary many different species when the subdivision ratio ζ varies. For example, the simplest one is bi-subdivision of the interval $[ll, ul]$; the interval $[ll, ul]$ can of course be subdivided by other subdivisions. For example, subdividing the interval by the *golden-ratio* is more efficient to the cases that $N_{(0,0)}=pq$ when q/p is close to the golden-ratio. Theoretically, the more sub-intervals are obtained, the faster the algorithm works.

4.4 Numerical Experiments

Numerical experiments are made on a PC with an Intel Xeon E5450 CPU and 4GB memory via C++ gmp big number library. Experiment data originate from two sources. Some are small Mersenne and Fermat Numbers; some are taken from articles [6], [7] as well as part data in article [8]. Except for applying the two approaches introduced previously, Pollard' Rho approach is also adopted and programmed according the introduction in article [9]. Tables 1 and 2 list the experimental results. It can see that the subdivision and squeeze approach is averagely faster than the Pollard's Rho approach, which is averagely faster than the sequential approach.

Table 1. Experiments on Mersenne and Fermat Numbers

N	*Small Factor*	Searching Steps		
		Pollard's Rho Approach	Sequential Approach	Squeeze Approach
$M67=2^{67}-1$	193707721	144192996	96853861	3369307
$M71=2^{71}-1$	228479	142096	114240	1025
$M83=2^{83}-1$	167	133	84	3
$M97=2^{97}-1$	11447	8828	5724	1107
$M103=2^{103}-1$	2550183799	15573107	1275091900	834274116
$M109=2^{109}-1$	745988807	773948830	372994404	45325572
$M113=2^{113}-1$	3391	152	1696	969
$F5=2^{32}+1$	641	129	399	39
$F6=2^{64}+1$	274177	226958	137089	40050
$F9=2^{521}+1$	2424833	792700	1212417	162293
$F10=2^{1024}+1$	45592577	14690570	22796289	1990552
$F11=2^{2048}+1$	319489	222255	159745	14348

Table 2. Experiments on Some Big Integers

N's Factorization	Searching Steps		
	Pollard's Rho	Sequential Approach	Squeeze Approach
N1= 1123877887715932507=299155897×3756830131	*14883075*	*81331692*	*17061564*
N2=1129367102454866881=25869889×43655660929	*24844*	*1025702*	*1025702*
N3=2974231569940674843 7=372173423×79915205819	*110166759*	*307698549*	*1834479*
N4=35249679931198483=59138501×596052983	*1050136*	*5166741*	*5166741*
N5=208127655734009353=430470917×483488309	*145344556*	*12869593*	*12869593*
N6=331432537700013787=114098219×2904800273	*14216696*	*2605343*	*2605343*
N7=3070282504055021789=1436222173×2137748993	*313213032*	*157999996*	*61027776*
N8=3757550627260778911=16053127×234069700393	*4685327*	*14059073*	*3502182*
N9=2492881699809468 4879=347912923×71652460573	*32455214*	*235004315*	*30523926*
N10=1018833756343551 7819=70901851×143696355169	*29872327*	*667123*	*667123*
N11=160000000000000022950000000000003170601 = 2000000000000002559× 80000000000000001239	*No result in a week*	*No result in a week*	*562*
N12=240000000000000090781000000000042854447 =23×1043478260869565612091304347826105588 89 =57×421052631578947527685964912280709272 71	*1*	*2*	*1*
N13=3795660161607007376406398635316376867773 =29×1308848331588623233243585736315992023 37	*16*	*23*	*4*

IV. CONCLUSIONS AND FUTURE WORK

As stated in article [1], putting odd numbers on a binary tree is a new approach to study integers and it can derive odd numbers' many new properties. Like the results derived in this article and in articles [1] and [2], the new properties do disclose odd numbers' many traits that have been rarely known before and are very useful in studying and analyzing integers. It can see from this article and the numerical experiment that the new properties of odd numbers can also provide new approaches to factorize integers. It is sure that, combined with other kinds of algorithms, such as the algorithms in articles [7] and [8], the new approach can reach an expected efficiency. And this will give valuable guidance to future work.

ACKNOWLEDGEMENTS

The research work is supported by the national Ministry of science and technology under project 2013GA780052, Department of Guangdong Science and Technology under projects 2015A030401105 and 2015A010104011, Foshan Bureau of Science and Technology under projects 2016AG100311, Special Innovative Projects 2014KTSCX156, 2014SFKC30 and 2014QTLXXM42 from Guangdong Education Department. The authors sincerely present thanks to them all.

REFERENCES

[1] WANG Xingbo, "*Valuated Binary Tree: A New Approach in Study of Integers*", International Journal of Scientific and Innovative Mathematical Research (IJSIMR), 4(3), 63-67(2016)(DOI:10.20431/2347-3142.0403008)

[2] Xingbo WANG, "*Amusing Properties of Odd Numbers Derived From Valuated Binary Tree*", IOSR Journal of Mathematics, 12(6,Ver.V),53-57(2016)(DOI: 10.9790/5728-1206055357)

[3] WANG Xingbo, "*New Constructive Approach to Solve Problems of Integers' Divisibility*", Asian Journal of Fuzzy and Applied Mathematics, 2(3),74-82(2014)

[4] Wang Xingbo, "*A* mean-value *formula for the* floor function on *integers*", Mathproblems Journal, 2(4),136-143(2012)

[5] WANG Xing-bo, "*Some supplemental properties with appendix applications of floor function*", Journal of Science of Teachers College and University (In Chinese),34(2),8-9(2014)

[6] R Sherman Lahman, "*Factoring Large Integers*", Mathematics of Computation, 28(126), 637-646(1974)

[7] ShaohuaZhang, GongliangChen, ZhongpingQin, et al, "A Method of Factoring Large Integers",Information Security and Communication privacy, (7),108-109(2005)

[8] ZHANG Shu-mei,SONG Wei-tang and SONG Wan-li, "*Discussion on Mantissam ultiphase particle swarm optimization applied to large integer factorization problem*",Computer Engineering and Applications,46(25),105-108(2010)

[9] Sonal Sarnaik, Dinesh Gadekarand Umesh Gaikwad, "*An overview to Integer factorization and RSA in Cryptography*",INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY,2(9),21-26,2014

[10] Xingbo WANG. "*Seed and Sieve of Odd Composite Numbers with Applications In Factorization of Integers"*, OSR Journal of Mathematics (IOSR-JM), 12(5, Ver. VIII), 01-07(2016)

[11] Xingbo WANG, "*Factorization of Large Numbers via Factorization of Small Numbers*", Global Journal of Pure and Applied Mathematics, 12(6), 5157-5173 (2016)